Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Previously Withdrawn) A method of generating a digital signature within a computer chip, comprising receiving data representing a message and generating a digital signature for the message by: (a) modifying the message data with additional data, and (b) then encrypting said modified message data using a private key of a public-private key pair stored within the computer chip.

2. (Previously Withdrawn) A method of generating a digital signature within a computer chip, comprising receiving data representing a message and generating a digital signature for the message by: (a) modifying the message data by appending additional data thereto, (b) calculating a hash value of said modified message data, and (c) then encrypting said calculated hash value using a private key of a public-private key pair.

3. (Previously Withdrawn) The method of claim 2, wherein said step of modifying comprises appending the additional data to the message data.

4. (Previously Withdrawn) The method of claim 2, wherein said step of modifying comprises embedding the additional data within the message data.

5. (PreviouslyWithdrawn) The method of claim 2, wherein the additional data comprises data prestored within memory of the computer chip.

6. (Previously Withdrawn) The method of claim 2, wherein the additional data represents a verification status of the device.

7. (Previously Withdrawn) The method of claim 2, wherein the message data includes a field identifier corresponding to a field of data prestored within the memory of the computer chip, the field identifier having a null value, and wherein said step of modifying the message data comprises retrieving the value stored in the memory location identified by the field identifier and embedding said retrieved value in the message data with the field identifier.

8. (Previously Withdrawn) The method of claim 7, wherein the memory of the computer chip in which the additional data is stored is content searchable memory.

9. (Previously Withdrawn) The method of claim 7, wherein the message data comprises XML formatting.

10. (Previously Withdrawn) A method for extracting user information from a computer chip, the computer chip including content searchable memory in which different fields of data are prestored, comprising transmitting an identifier of a particular field of data prestored within the computer chip together with a null value therefor.

11. (Previously Withdrawn) The method of claim 10, wherein the identifier and null value therefor transmitted to the computer chip comprise XML formatting.

12. (Currently Amended) A method for providing a random number for utilization in a computer program application that requires the random number for secure electronic communications, the method comprising:

creating a private key of a public/private key pair within a secure device;

generating, within the secure device, a verification status indicator based at least in part on a comparison of pre-stored verification data stored by the secure device to input verification data received from a user of the secure device, wherein the verification status indicator does not include the pre-stored verification data or the input verification data;

upon receipt of message data at the secure device, originating a digital signature for the message data, the originating comprising:

calculating a hash value for the message data;

encrypting at least the hash value using the private key; and

providing results of the ~~encrypting step~~ encryption as a generated digital signature; and

providing the generated digital signature and the verification status indicator to the computer program application,

wherein the computer program application is external to the secure device, and

wherein the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications.

13. (Previously Amended) The method of claim 12, further comprising using the generated digital signature as a random number to distinguish and prevent a replay attack.

14. (Previously Amended) The method of claim 12, further comprising using the generated digital signature to generate a session key for secure electronic communications.

15. (Previously Amended) The method of claim 12, wherein the digital signature is generated within a computer chip within the secure device.

16. (Previously Amended) The method of claim 15, wherein the computer chip itself includes a random number generator.

17. (Previously Amended) The method of claim 16, wherein the digital signature is generated within the computer chip using the private key and a random number obtained from the random number generator.

18. (Original) The method of claim 17, wherein an elliptical curve digital signature algorithm is utilized to generate the digital signature.

19. (Original) The method of claim 18, wherein the random number generator is directly inaccessible from outside of the computer chip.

20. (Original) The method of claim 18, wherein the random number generator is accessible only by a digital signature circuit.

21. (Currently Amended) A secure device for providing a random number for utilization within a computer program application that requires the random number for secure electronic communications, the secure device comprising:

a user interface for receipt of verification data and message data;

a verification component that generates a verification status indicator based at least in part on a comparison of pre-stored verification data stored by the secure device to the received verification data, wherein the verification status indicator does not include the pre-stored verification data or the received verification data;

a memory means for the storage of a private key of a public/private key pair and the pre-stored verification data;

a digital signature component in communication with the memory means, wherein

the digital signature component originates a digital signature for the message data, the origination comprising:

calculation of a hash value for the message data;

encryption of at least the hash value using the private key; and

provision of the encryption results as a generated digital signature; and

an output means for providing the generated digital signature and the verification status indicator to the computer program application, wherein the computer program application is external to the secure device, and wherein the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications.

22. (Previously Amended) The secure device of claim 21, further comprising means for using the generated digital signature as a random number to distinguish and prevent a replay attack.

23. (Previously Amended) The secure device of claim 21, further comprising means for using the digital signature to generate a session key for secure electronic communications.

24. (Previously Amended) The secure device of claim 21, further comprising a computer chip for generation of the digital signature.

25. (Previously Amended) The secure device of claim 24, wherein the computer chip further comprises a random number generator.

26. (Previously Amended) The secure device of claim 25, wherein the digital signature is generated within the computer chip using the private key and a random number obtained from the random number generator.

27. (Previously Amended) The secure device of claim 26, wherein an elliptical curve digital signature algorithm is utilized to generate the digital signature.

28. (Previously Amended) The secure device of claim 27, wherein the random number generator is directly inaccessible from outside of the computer chip.

29. (Previously Amended) The secure device of claim 27, wherein the random number generator is accessible only by a digital signature circuit.

30. (Previously Presented) The method of claim 12, wherein the computer program application is a security protocol.

31. (Previously Presented) The method of claim 30, wherein the security protocol is a secure socket layer (SSL) protocol.

32. (Previously Presented) The method of claim 30, wherein the security protocol is a pretty good privacy (PGP) protocol.

33. (Previously Presented) The method of claim 12, wherein the computer program application is a digital signature algorithm for generating a digital signature.

34. (Previously Presented) The secure device of claim 21, wherein the computer program application is a security protocol.

35. (Previously Presented) The secure device of claim 34, wherein the security protocol is a secure socket layer (SSL) protocol.

36. (Previously Presented) The secure device of claim 34, wherein the security protocol is a pretty good privacy (PGP) protocol.

37. (Previously Presented) The secure device of claim 21, wherein the computer program application is a digital signature algorithm for generating a digital signature.

38. (Previously Presented) The method of claim 12, wherein the message data is modified by the verification status indicator prior to originating the digital signature, and

wherein the verification status indicator is provided to the computer program application as a component of the generated digital signature.

39. (Previously Presented) The secure device of claim 21, wherein the digital signature component modifies the message data with the verification status indicator prior to originating the digital signature, and

wherein the output means provides the verification status indicator to the computer program application as a component of the generated digital signature.